한국컴퓨터정보학회 동계학술대회 논문집 제24권 제1호 (2016. 1)

통신 호 네트워크 구간 암호화를 통한 스마트폰 통신 보안 전송 기법

배기태*, 정민영**
*서울미디어대학원대학교 뉴미디어경영학과
**광주여자대학교 실버케어학과
e-mail:ktbae@smit.ac.kr*, myjeong@kwu.ac.kr**

A Study on Smart Phone Communication Security Using AES256 Encryption

Ki-Tae Bae*, Hyeok-Gyu YunO
*Dept. of Newmedia Business, Seoul Media Institute of Technology
**Dept. of Silver Care, Kwangju Women's University

● 요 약 ●

본 논문에서는 스마트폰의 폭발적 증가와 함께 스마트폰의 악성코드 및 해킹 도구에 의해 스마트폰의 음성, 문자, 데이터 도청이 문제가 되고 있으며 최근 [1]"미국 NSA가 35개국 정상 전화 도청 사건"에 이르기 까지 도청은 국가사회적 문제로 발단 되고 있다. 본 연구에서는 통신 호 사이의 네트워크에 전송되는 음성, 문자, 데이터를 [2]"AES256 암호화 알고리즘"을 통해 암호화하여 도청을 방지하고 AES256 암복호화를 송수신 스마트폰에서 수행하여 통신 호 사이 네트워크 구간의 부하를 줄임으로써 암복호화에 따른 네트워크 구간의 성능 저하 문제를 해결하고자 한다.

키워드: 스마트폰 보안(SmartPhone Security), AES256암호화(Encryption), 모바일 통신Communication)

I. Introduction

정보화기기가 스마트폰의 폭발적 증가와 동시에 스마트폰의 악성코드 증가 수가 2015년 상반기 10만개 이상이 발견되고 있으며 이는 2015년 상반기 대비 100배 이상 증가한 수치로 실로 심각한 문제로 대두 되고 있다. 특히 안드로이드 운영체제가 절대적으로 시장을 점유하고 있는 상황에서 안드로이드 운영체제의 보안에 대한 연구는 활발히 진행되고 있다.

본 연구는 안드로이드 기반 스마트폰에 AES256 암호화 알고리즘을 사용해 스마트폰 통신 호 네트워크 구간에 대하여 음성, 문자, 데이터 도청 방지 및 보안을 목적으로 하는 연구로 이를 통해 개인의 사생화 보호 및 정보 유출 방지 등의 기대효과를 가져올 수 있다.

II. 본론

1. 시스템 구성도

[그림1]은 두 단말기 사이 통신 호 네트워크 상의 AES256암호화가 적용되어 사용되는 것을 볼 수 있다. 송신 단말기에 발생되는 음성, 문자, 데이터를 AES256 암호화 앱을 통하여 암호화 하며 수신 단말기에서 AES256 복호화 앱을 통해 음성, 문자, 데이터를 복호화하여 내용을 수신할 수 있다. 하지만 수신 단말기에 복호화 값이 없는 단말기의 경우 암호화 된 문자 데이터를 수신하여 내용을 알 수 없으며 음성 또한 알 수 없는 음성으로 전달된다.

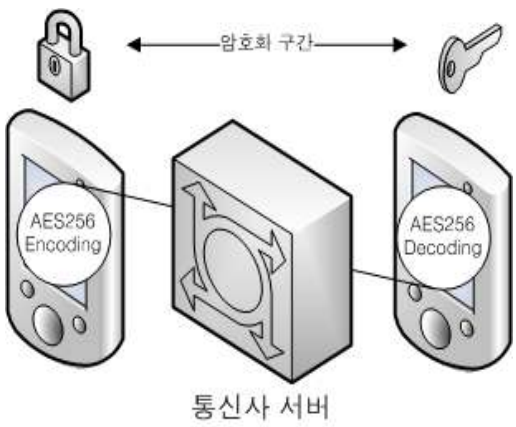

Fig. 1. The Overall Process of System

핵심 내용은 송수신 두 단말 사이에 AES256 암호화 데이터가 전송되기 때문에 "tower spoofing" 즉, 해킹을 위해 기지국 속이기를 통한 도청 및 휴대용 도청장치 등을 이용하여 [그림1]의 암호화 구간을 도청하더라도 AES256 암호화로 인해 도청이 불가능 하게 되나.

2. 암호화 통신 방법

[그림2]에서와 같이 보안 통신을 위하여 두 가지 방식을 생각할 수 있다. 우선 문자 메시지의 경우 스마트폰에서 encoding 및 decoding을 직접 수행하여 발송하기 때문에 특별히 관리/인증/보안 서버를 거칠 필요가 없이 직접 발송 할 수 있으며 두 번째 음성, 데이터의 경우 음성, 데이터 용량 처리를 위하여 별도의 관리/인증/보안서버를 두어 이곳에서 암호화 및 voip 통신 처리를 수행한다. 스마트폰에서는 암복호화키를 가지고 있어 관리/인증/보안 서버와 통신하여 암복호화를 위한 키 값을 전달해 준다.

Fig. 2. Security Communication

3. 실험 및 결과

본 실험에서는 송신기에서 동일 내용의 문자 메시지를 암호화하여 전송하고 복호화 키가 있는 수신기와 복호화 키가 없는 수신기에서 각각 문자 메시지를 수신할 경우에 대한 실험 환경을 구성한다.실험을 위하여 안드로이드 운영체제가 설치된 단말기 3대를 준비하고 안드로이드 운영체제에서 AES256 암복호화 App을 개발하여 송신기1대와 수신기1대에 개발한 App을 설치한다. 나머지 1대는 설치하지 않는다. [그림3]와 같이 송신기에서 문자 메시지를 작성하여 수신기 2대로 동시에 전송한다. 송신기 App에서 AES256으로 암호화한 후 문자가 전송되어 2대의 수신기에서 받은 문자 내용을 확인해 본다. 그림 3과 같이 복호화 App이 설치되지 않은 수신기1에서 는 암호화된 문자 메시지를 확인 할 수 있으며 복호화 App이 설치된 수신기2는 정상적인 문자 메시지를 확인 할 수 있다.

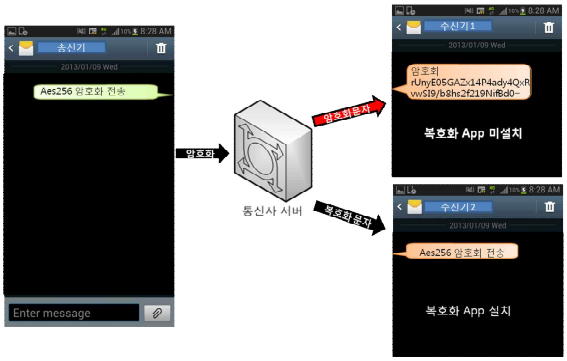

Fig. 3. Test Result

III. 결론

스마트폰의 폭발적 증가와 더불어 악성코드 수의 증가로 도청 및 보안에 대한 문제가 사회적 이슈로 떠오르고 있으며 이를 해결하려는 노력이 각계에서 이루어지고 있다. 본 논문에서는 AES256 암호화 방법을 사용하여 스마트폰의 음성, 문자, 데이터 암호화 전송을 통해 도청 및 보안 문제를 해결하기 위한 시스템을 제안하였다. 제안한 시스템에 MDM(Mobile device management) 등의 부가 서비스를 추가하여 보안 서비스적 활용도를 높일 수 있을 것이라 기대된다.

References

[1] Douglas R. Stinson, 《Cryptography Theory and Practice 3rd edition》, Chanpman & Hall/CRC, 2006, pp. 102-103.

[2] Makatchev, M., & Wada, M. (2000). Formative behavior network for a biped robot; 9th IEEE International Workshop on Robot and Human Interactive Communication, (pp. 101-106). September 27-29, Osaka, Japan.